AJ.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,941	07/25/2001	Michael L. Wenocur	A-70559/RMA	7253

7590 01/26/2005

FLEHR HOHBACH TEST ALBRITTON & HERBERT, LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111

EXAMINER	
BLAIR, DOUGLAS B	
ART UNIT	**PAPER NUMBER**
2142	

DATE MAILED: 01/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,941	WENOCUR ET AL.	
	Examiner	Art Unit	
	Douglas B Blair	2142	

-- The MAILING DATE of this communication appears on the cover sheet with th correspondence address --

Period for R ply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/19/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 2, and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 1 recites the limitation "its own Subject Name" in line 15 of the claim. It is unclear whether "its" refers to the client or the Resource Tag. There is insufficient antecedent basis for this limitation in the claim.

4. Claim 1 recites the limitation "the same protocol" in line 19 of the claim. It is unclear what the protocol is supposed to be the same as. There is insufficient antecedent basis for this limitation in the claim.

5. Claim 1 recites the limitation "the Client's Subject Name" in line 22 of the claim. There is insufficient antecedent basis for this limitation in the claim.

6. Claim 1 recites the limitation "the public key(s)" in line 30 of the claim. There is insufficient antecedent basis for this limitation in the claim.

7. Claim 2 is rejected for the same reasons as claim 1.

8. Claim 26 recites the limitation "the method of claim 2" in line 1 of the claim. There is insufficient antecedent basis for this limitation in the claim.

9. Claim 26 recites the limitation "as explained earlier" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 5,717,759 to Micali in view of U.S. Patent Number 6,356,937 to Montville et al..

12. As to claims 1 and 2, Micali teaches the steps of extracting, by the client, a Resource Tag related to its own Subject Name from a message that was received from a Server; extracting, by the client, a public and private key and certificate chain from a trusted source (col. 4, line 54-col. 5, line 36); using the extracted information to create a secure session with the Issuer that authenticates the issuer using the same protocol (col. 4, line 54-col. 5, line 36); sending, by the client, as the client's first Data message after any session setup messages, a data structure that has a common header with fields for Type, Version, and Content-Length, and contents that include the Resource Tag, the Client's Subject Name, and optionally one or more public keys that the client has generated (col. 5, lines 37-67); verifying, by the certificate issuer, that a valid Server issued the Resource Tag and that the Resource Tag is valid for the given received Subject Name (col. 5, lines 37-67); creating, by the issuer, a Compact Certificate with one or more public keys and with the Client's Subject Name, digitally signing, by the issuer, the certificate with the Issuer's private key; and sending, by the certificate issuer, a message back to the Client over the secure channel, where the message includes the Compact Certificate and if the Issuer generated

the public key(s), the message includes the matching private key(s) (col. 5, lines 37-67); however Micali does not explicitly teach the subject name of being part of the certificate.

Montville teaches a Subject Name being part of a certificate (col. 11, line 56-col. 12, line 6).

It would have been obvious to one of ordinary skill in the Computer Networking art at the time of the invention to combine the teachings of Micali regarding the implementation of a certificate issuing system with the teachings of Montville regarding a Subject name being part of a certificate because binding the subject name improves security (Montville, col. 11, line 56-col. 12, line 6).

13. As to claim 3, Micali teaches a method further comprising the client placing the Compact Certificate and keys into its trusted source or storage means (col. 4, line 54-col. 5, line 36).

14. As to claim 4, Micali teaches a method wherein the one or more public key(s) are generated by the Issuer or send to the Issuer by the Client who generated them (col. 4, line 54-col. 5, line 36).

15. As to claim 5, Micali teaches a method wherein where the one or more public key(s) are sent to the Issuer by the Client who generated them (col. 4, line 54-col. 5, line 36).

16. As to claim 6, Micali teaches a method wherein the trusted source or storage means is data compiled into the Client software (col. 4, line 54-col. 5, line 36).

17. As to claim 7, Micali teaches a method wherein the trusted source or storage means is data received from communicating with a Server via a secure session (col. 5, lines 37-67).

18. As to claim 8, Micali teaches a method wherein the trusted source comprises a trusted storage (col. 4, line 54-col. 5, line 36).

19. As to claim 9, Micali teaches a method wherein the network address comprises a URL (col. 5, lines 37-67).

20. As to claim 10, Micali teaches a method wherein the Resource Tag comprises a message tag (col. 5, lines 37-67).

21. As to claim 11, Montville teaches a method wherein the Subject Name comprises an e-mail address (col. 11, line 56-col. 12, line 6).

22. As to claim 12, Micali teaches a method wherein the public and private key operations are performed by any asymmetric cryptosystems (col. 4, line 54-col. 5, line 36).

23. As to claim 13, Montville teaches a method wherein the asymmetric cryptosystem is selected from the group consisting of RSA, Elliptic Curve, and NTRU (col. 8, lines 37-47).

24. As to claim 14, Micali teaches a method wherein the public and private key extracted by the client are fixed public and private keys (col. 5, lines 37-67).

25. As to claim 15, Micali teaches a method wherein the public and private key and certificate chain extracted by the client are fixed public and private keys and certificate chain (col. 4, line 54-col. 5, line 36).

26. As to claims 16-26, they are rejected for the same reasons as claims 1-15.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas B Blair whose telephone number is 571-272-3893. The examiner can normally be reached on 8:30am-5pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jack Harvey can be reached on 571-272-3896. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Douglas Blair
DBB

JASON CARDONE
PRIMARY EX.
AU: 2145